

APPLICATION
FOR
UNITED STATES LETTERS PATENT

APPLICANT NAME: Michael T. White, et al.

TITLE: Enhanced Security Features for an Automated Order Fulfillment System

DOCKET NO.: FI9-99-140

INTERNATIONAL BUSINESS MACHINES CORPORATION

CERTIFICATE OF MAILING UNDER 37 CFR 1.10
I HEREBY CERTIFY THAT, ON THE DATE SHOWN BELOW
THIS CORRESPONDENCE IS BEING DEPOSITED WITH
THE UNITED STATES POSTAL SERVICE IN AN ENVELOPE
ADDRESSED TO THE ASSISTANT COMMISSIONER FOR
PATENTS, WASHINGTON, D.C. 20231 AS "EXPRESS MAIL
POST OFFICE ADDRESSEE"

MAILING LABEL # EK082874135US

ON December 22, 1999

RobinAnn Zeno

Name of person mailing paper

RobinAnn Zeno 12/22/99
Signature Date

ENHANCED SECURITY FEATURES
FOR AN AUTOMATED ORDER FULFILLMENT SYSTEM

FIELD OF THE INVENTION

5 This invention relates to improvements in an automated system for managing fulfillment of customer orders, and more particularly to security enhancements to prevent fraud by system users.

BACKGROUND OF THE INVENTION

10 A number of processes related to the fulfillment of customer orders lend themselves to automation. For example, systems have been developed for (1) scheduling the shipment of goods to a customer and (2) managing customer accounts payable. More recently, an integrated system for managing the fulfillment of orders has become available. An example of such an integrated system is the SAP™ system ("Systems, Applications, Products and Data Processing") offered by SAP AG, Walldorf, Germany.

15 Security functions in separate materials management and customer accounts-payable systems, providing safeguards against fraud and inappropriate business practices, can be inadequate when those systems are integrated (for example, into the SAP system). Each user (known to the system by his user ID) has a "security profile" listing the transactions he may approve or the tasks he is authorized to perform. Some of these transactions are incompatible, in the sense that having them

under control of a single individual could result in abuse of the system. For example, a user authorized both (1) to approve the shipment of goods to a certain customer and (2) to adjust the amount owed by a customer, could fraudulently ship goods to himself free of charge. Furthermore, an individual with a single user ID but multiple security profiles could initiate a transaction under one profile, then instruct the system to perform an incompatible transaction appearing under another profile.

Accordingly, there is a need for improved security in an automated system for managing the fulfillment of orders, whereby the security profiles of users are analyzed and modified to prevent incompatible transactions by those users.

SUMMARY OF THE INVENTION

The present invention provides a system for the separation of incompatible transactions within a system such as the SAP system, so that critical tasks (those tasks susceptible to abuse or fraud) may be assigned to different individuals. In accordance with the invention, this system determines which transactions in a user's security profile are incompatible with each other, and then generates a report indicating the security profile which has incompatible transactions. The security profiles may then be modified, to prevent inappropriate business conduct including fraud and misuse of funds.

According to a first aspect of the present invention, a method is provided which includes the steps of assigning a user identifier to each user of the system; preparing a security profile corresponding to each identifier, where each security profile includes a set of authorized transactions; and preparing a list of pairs of incompatible transactions in accordance with predetermined rules of business conduct. Then,

according to this method, each security profile is compared with that list, to identify security profiles including at least one pair of incompatible transactions. A report is generated indicating those security profiles which include incompatible transactions and the user identifiers associated with those security profiles. If a security profile is found to have a pair of incompatible transactions, it may be modified; alternatively, the list of pairs of incompatible transactions may be modified, so that the security profile does not include a pair of incompatible transactions. Another report may then be generated indicating the modification made.

A given user identifier may have more than one security profile associated therewith. In accordance with a second aspect of the invention, a method is provided which includes the steps of assigning a user identifier to each user of the system; preparing a plurality of security profiles, where each user identifier is associated with at least one security profile; and preparing a list of pairs of incompatible transactions in accordance with predetermined business conduct rules. Furthermore, the method includes the steps of generating a set of transactions in all of the security profiles associated with each user identifier, and comparing that set of transactions with the list of pairs of incompatible transactions. This method therefore permits identification of user identifiers having associated therewith at least one pair of incompatible transactions, even if those transactions are in different security profiles. A report is then generated indicating those user identifiers. A security profile associated with such a user identifier may be modified; alternatively, the list of pairs of incompatible transactions may be modified, so that the user identifier no longer has a pair of incompatible transactions associated therewith. Another report may then be generated indicating any modification which has been made.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic block diagram of a computer system on which software embodying the present invention is loaded, and which includes a storage device for storing user IDs, security profiles, and transaction tables used in accordance with the present invention.

Figure 2A illustrates in tabular form the structure of the user ID database.

Figure 2B illustrates in tabular form the structure of the security profile database.

Figure 3A illustrates the structure of a table of critical transactions.

Figure 3B illustrates the structure of a table of incompatible critical transactions.

Figure 4 is a flowchart showing a method for analyzing security profiles and generating a report of incompatible transactions in a profile, according to a first embodiment of the present invention.

Figures 5A and 5B are connected flowcharts showing a method for analyzing security profiles associated with a given user ID and generating a report of incompatible transactions for that user, according to a second embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 is a block diagram of a computer system 100 on which is loaded a system 101 for managing fulfillment of orders (e.g. the SAP system) which includes a system 110 for separating critical tasks or transactions among various system users, according to the present invention. The computer system 100 also includes a storage device 120, in

which is stored a table 121 of user IDs for the system 101; security profiles 122 comprising lists of specific critical transactions; and tables 123 of critical transactions and combinations of incompatible transactions. The systems 101 and 110 access these tables, as shown schematically in Figure 1.

The storage device 120 may be an integral part of the computer system 100, as shown in Figure 1, or may be external to it. The executable code for the system 110 and the databases 121-123 may be stored on a variety of possible computer-readable media (RAM, ROM, CD-ROM, etc.).

The system 110 of the present invention is shown in Figure 1 as integrated into the commercially available system 101 for managing fulfillment of orders. Alternatively, the system 110 may be separate from system 101, or be invoked as a subroutine from system 101 (in which case the analysis of critical transactions may itself be viewed as a critical transaction, to be performed only by certain selected users). The user IDs 121, profiles 122 and tables 123 contain information used in the analysis, as detailed below.

As shown in Figure 2A, each user of the system 101 is assigned one record in the user ID database 121. Each record has fields 201 and 202 for the user ID and user name respectively, and a field 203 identifying the security profile or profiles assigned to that user. A given user may have a unique or custom-designed profile (for example, profile #1 in Figure 2A), have a single standard profile (such as profiles #2 and #3), or may be assigned multiple profiles. The database of security profiles is shown in Figure 2B. Each profile identifier is associated with a group of critical transactions; the identifiers for the transactions in a given profile are listed in field 204. In this illustration, the transactions are identified by a four-character code. A system user with a given user ID is

authorized to perform any of the transactions in the profile or profiles assigned to his user ID.

5 The profiles are constructed and analyzed using tables 123-1 and 123-2 of critical transactions and incompatible combinations thereof, as shown in Figures 3A and 3B. Figure 3A shows the structure of table 123-1, which has a list of all the critical transactions performed in system 101. Only the critical transactions--that is, those susceptible to abuse or fraud--need be listed in table 123-1. Each record of table 123-1 has the identifier 205 of the transaction, and the name of the transaction 206. Table 123-2, which is developed manually using the organization's rules and instructions (e.g. corporate "Business Conduct Guidelines"), lists combinations of critical transactions deemed incompatible: transactions which, if performed by the same user, would permit misuse of the system or fraud. Each record 301 of this table has the identifiers of two transactions which should not appear in the same security profile, or in a set of security profiles belonging to a particular system user.

15 In the following embodiments of the invention, the processes of identifying and tabulating incompatible transactions are not fully automated. It will be appreciated that these processes depend upon an understanding of both the order-fulfillment management system and the business-conduct ethics governing the organization using the system. These particular processes require a level of professional judgment in accordance with generally accepted accounting practices ("GAAP"), which then are implemented by a human system administrator.

25 A flowchart of a method of analyzing a security profile, according to a first embodiment of the invention, is shown in Figure 4. In step 401, the table 122 of security profiles is built and stored in memory. In step 402, the combinations of

critical transactions which are incompatible are identified. In a corporate environment, the corporate rules and instructions 450 serve as input for this step. The table 123-2, which lists all the combinations of incompatible transactions, is then built (step 403).

The identifier 203 of the profile to be analyzed is input by the system administrator, and this profile is retrieved from memory (step 404), and the transactions associated with that profile are compared with the table 123-2 (step 405). The results of this comparison (step 406) are included in a report (here referred to as Report #1). If no conflicting transactions exist in the profile, the report states that result (step 407). If one or more pairs of conflicting transactions are found, these are listed in the report (step 410). At this point (step 411), the person performing the analysis may modify the profile or the table 123-2 to remove the conflict between transactions. Alternatively, he may choose to allow the conflicting transactions to remain in the profile, and prepare a memo to management justifying this course of action.

It will be appreciated that these steps may be performed using an incomplete profile, so that the profile may be built without having incompatible transactions. In particular, it is desirable to analyze the profile (and make any necessary adjustments) while the order-fulfillment management system is in development, before it is moved to a production environment.

According to a second embodiment of the invention, another report (termed Report #2) is generated in connection with the analysis shown in the flowcharts of Figures 5A and 5B. Using a user ID as input, this report lists all of the transactions that are in conflict across all the profiles associated with that user ID. In steps 501-503, the tables 122 and 123-2 are built, as described above with reference to

steps 401-403.

5 In accordance with input from the system administrator,
a user ID is retrieved from the user ID database 121 (step
504), and a profile associated with that user ID is retrieved
from database 122 (step 505; see Figures 2A and 2B).
However, a particular user may be authorized to perform tasks
or approve transactions from more than one security profile.
All of the profiles associated with that user ID are
retrieved (steps 505-507), and the transactions of those
10 profiles are collected in a single, temporary list which is
compared with the list of incompatible transactions in table
123-2 (step 508). Accordingly, all incompatible transactions
belonging to a user ID are identified, whether that user ID
has a single security profile or multiple profiles.

15 If the user ID does not have any profiles with
incompatible transactions, Report #2 states that result (step
510). If, however, a set of incompatible transactions is
found (step 509), those transactions are listed in Report #2
(step 511), along with the user ID and the profile(s) in
20 which the transactions appear. As in the first embodiment,
the person performing the analysis may take a number of
actions to resolve the presence of incompatible transactions
(step 521): modify the profile, modify the table 123-2, or
justify the continuance of conflicting transactions belonging
25 to the user ID.

It is desirable to produce another report (Report #3)
which provides an audit trail; that is, a report listing all
the activity that has occurred against the transaction table
123-2. Thus if the system administrator intervenes to remove
30 a conflict in a security profile, this action will be
documented (step 601 in Figures 4 and 5B).

It will be appreciated that this procedure may be used
when developing and testing a set of profiles for a system
user. In that event, a dummy user ID with those profiles

